REMARKS

Favorable reconsideration of this application, in light of the preceding amendments and following remarks, is respectfully requested.

Claims 21-28, 30-32, and 34-40 are pending in this application. By this Amendment, claims 21 and 39 are amended; and claims 29 and 33 are cancelled without prejudice to or disclaimer of the subject matter contained therein. No new matter is added. Claims 21 and 39 are the independent claims.

Objection to the Claims

Claims 1 and 39 are objected to because of informalities. Applicants have amended claims 1 and 39 taking into consideration the Examiner's comments, to obviate the objection. Withdrawal of the objection is respectfully requested.

Claim Rejections - 35 U.S.C. § 103

Claims 21-40 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,864,757 to Parker ("Parker") in view of U.S. Patent Publication No. 2002/0186845 to Dutta et al. ("Dutta"). Applicants respectfully traverse this rejection for the reasons discussed below.

In order to establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), all of the claim limitations of the rejected claims must be described or suggested by the cited document(s).[1] Applicants respectfully submit that the cited documents do not meet this criterion, because no combination and/or modification of the Parker and

[1] See *In Re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). See also MPEP § 2143.03.

Dutta references will describe or suggest all of the claim limitations of rejected claims 21-40, and therefore, a *prima facie* case of obviousness has not been established.

For example, claim 21, as amended, recites, a method for managing security of at least one additional application associated to a main application with a security module of an equipment connected, via a network, to a control server managed by an operator, the main application and the additional applications use resources as data or functions stored in the security module locally connected to said equipment, the method being carried out on at least one of each initialization, activation or deactivation of the at least one additional application, comprising, *inter alia*:

> selectively activating or deactivating at least one resource as data or functions stored in said security module by executing the instructions included in the cryptogram and using the selected resource to condition the functioning of the at least one additional application stored in the equipment according to criteria established by at least one of a supplier of said additional application, the operator and a user of the equipment,
>
> wherein the resources as data or functions of the security module used by the main application are left active for connection of the equipment to the network so as to obtain further cryptograms from the control server. (*emphasis added*)

Applicants respectfully submit that the Parker and Dutta references do not disclose or suggest the above features.

In the outstanding Office Action, the Examiner admits that Parker fails to disclose or suggest the features of "selectively activating or deactivating at least one resource as data or functions stored in said security module.....the resources as data or functions of the security module used by the main application are left active for connection of the equipment to the network so as to obtain further cryptograms from

the control server."[2] Yet, the Examiner attempts to remedy the admitted deficiencies of Parker by asserting that Dutta teaches the above features. Applicants respectfully disagree.

In particular, Parker discloses a method for locking/unlocking a mobile terminal, or more precisely, a subscriber module such as a SIM card to services provided by a predetermined operator. A message is sent by the operator to the security module via the mobile terminal to deactivate or activate the whole security module, so that the terminal state is either, unlocked, locked or limited to emergency calls (*see, e.g., col. 3, lines 49-59).*

Moreover, claim 21 recites that the resources as data or functions of the security module used by the main application are kept active for maintaining connection to the control server allowing the equipment to receive further cryptograms. The latter includes instructions in which execution acts on security module resources used by one or several additional applications. See, e.g., paragraph [0023] at page 7 of the instant disclosure, in that:

> "*...According to the type of realization, it is possible that certain resources of the subscriber module used by low security level applications are implemented by default before the arrival of the cryptogram. This is also the case for resources necessary to obtain access to the network, without this the sending of the cryptogram would not be possible by this same network.*"

The cell phone of Parker, however, includes only one application having the main feature of the "calling function." This application may have one of the three statuses as unlocked, locked and limited to emergency calls according to commands sent by the control server.

---

[2] See Office action mailed July 19, 2010, page 4, 6th paragraph.

Accordingly, using of resources as data or functions of the security module managing the main application as well the additional application is not mentioned by Parker. The cell phone of Parker has only one application which may be locked, unlocked or limited to emergency calls only. The notion of selectively activating or deactivating security module resources is therefore not disclosed in Parker since, in claim 21, the selection may be performed by the security module on resources of specific additional applications according to instructions of the cryptogram. This action may be performed without disabling the main application resources which are necessary for connection of the equipment to the network.

Further, the mode "emergency calls only" cannot be considered as an application in itself or is considered an additional application because it is a special function of the main application set in case of codewords mismatch (*see, e.g., col. 10, lines 64-67, col. 11, lines 1-5 of Parker*).

Therefore, Applicants submit that Parker fails to disclose or suggest, *inter alia*, "resources as data or functions of the security module used by the main application are left active for connection of the equipment to the network so as to obtain further cryptogram from the control server," as recited in claim 21.

In regard to the Dutta reference[3], this reference merely discloses a method for remotely controlling a security element of a mobile terminal by disabling access to secured functions. When a user wishes to remotely disable a function of the terminal,

[3] To be thorough, further expedite prosecution, and for the sake of clarity, Applicants provide discussions of each of the references separately, however, Applicants are not attacking these references individually, but arguing that the references, even taken in combination, fail to render the claimed invention obvious because all features of claim 21 are not found in the prior art.

the user accesses the service via the telephone network, Internet, Email, or other means. A server of the service provider verifies authenticity of the user, and creates a signed message including, at least, an address for the mobile terminal and instructions for disabling the application to be executed on the mobile terminal. The service provider then sends the message to the mobile terminal and the mobile terminal can respond with an authenticated confirmation message. Disabled functions thus can be re-enabled by an appropriate message sent by the service provider upon request from the user in a similar way than for disabling functions.

The operation of controlling the security element in Dutta is always initiated upon user request while, in contrast, claim 21 recites that the management of the application security is performed by the control server. In fact, the control server "automatically" receives identification data and manages security of the additional applications at specific opportunities. For instance:

- at least one of each initialization, activation or deactivation of the at least one additional application,
- after each connection of the mobile equipment to the network,
- after each updating of the software version of the mobile equipment,
- after each updating of the software version of the subscriber module,
- after each updating of the resources on the subscriber module, and/or
- periodically at a rate given by the control server.

These opportunities are not managed by a request or a command sent by the user as in Dutta, but depend mainly on the current status of the additional applications installed in the terminal.

Accordingly, Applicants respectfully submit that a solution for managing automatic conformity of an application, software version of the application, terminal or security module, resources of the same by specific instructions from the control server can thus not be found in the proposed combination of Parker and Dutta.

Since the rejection fails to disclose or suggest each and every element of the rejected claims, Applicants respectfully submit that no *prima facie* case of obviousness has been established with respect to claim 21.

Further, in order to establish a *prima facie* case of obviousness, the Examiner must establish that it would have been obvious for one of ordinary skill to have combined the teachings of the cited documents.[4] One way to establish this would be to show "some articulated reasoning with some rationale underpinning to support the legal conclusion of obviousness" and "identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does."[5] Furthermore, the Examiner must make "*explicit*" this rationale of "the apparent reason to combine the known elements in the fashion claimed," including a detailed explanation of "the effects of demands known to the design community or present in the marketplace" and "the background knowledge possessed by a person having ordinary skill in the art."[6]

It is respectfully submitted that the Examiner has not met these criteria. For example, the Examiner asserts that:

> it would have been obvious to one of ordinary skill in the art at the time the invention to combine the teaching of Dutta with those of Parker to give service provider control over not only the calling functions of a cell phone but also the applications running

---

[4] See *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. at 398, 82 USPQ2d at 1396 (2007).
[5] *Id.*
[6] *Id.*

> on them in order to safeguard the SIM data. Deactivating just the security functions allows the phone to stay on the network, send acknowledgements of the remote commands, and report its location.

However, it is respectfully submitted that the above statement is merely conclusory and do not comprise an "*explicit rationale*" as required by *KSR Int'l*. Therefore, because the Examiner has not provided an explicit analysis as required by *KSR Int'l*, a *prima facie* case of obviousness has not been established.

In view of the above, Applicants respectfully submit that the Parker and the Dutta references, individually or in combination, fail to teach or suggest each and every element of claim 21, and therefore, claim 21 is allowable over the cited prior art. Claim 39 is also allowable for the similar reasons discussed above regarding claim 21. Specifically, claim 39 recites, *inter alia*, "a security module including resources as data or functions intended to be locally accessed by a main application and at least one additional application installed in an equipment connected, via a network, to a control server configured for managing security of the at least one additional application on at least one of each initialization, activation or deactivation of the at least one additional application."

Claims 22-28, 30-32, 34-38, and 40 are dependent from either claims 21 or 39, and therefore, also allowable. Accordingly, Applicants respectfully request that the rejection under 35 U.S.C. § 103(a) be reconsidered and withdrawn.

Request for Interview

Applicants respectfully request, prior to the issuance of an action on the merits, that the Examiner grant an interview (telephonic or in-person) with Applicants' representative in order to discuss the Office Action, and the differences between the cited prior art and the subject matter cited in the claims.

CONCLUSION

In view of the above remarks and amendments, Applicants respectfully submit that each of the pending objections and rejections has been addressed and overcome, placing the present application in condition for allowance. A notice to that effect is respectfully requested. Further, the above remarks demonstrate the failings of the outstanding rejections, and are sufficient to overcome the rejections. However, these remarks are not intended to, nor need they, comprehensively address each and every reason for the patentability of the claimed subject matter over the applied prior art. Accordingly, Applicants do not contend that the claims are patentable solely on the basis of the particular claim elements discussed above.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact the undersigned, at the telephone number below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

John A. Castellano, Reg. No. 35,094

P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JAC/DJC:has
1009828.1